



ATTACHMENT B Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A computer system comprising at least one computer with a processor operating under the control of a program, operating on input data items each suitable for being associated with a code so as to provide input data codes and supplying output data items each suitable for being associated with a code and for being transmitted or applied to output members, the system being characterized by at least one peripheral external to the processor, connected to the processor to receive at least the input data codes, the operands, and the nature of the operation for each elementary operation performed by the processor, the processor and the at least one peripheral both processing all types of said input data codes, the peripheral having secure architecture and computing a code for each elementary operation performed by the processor and verifying proper operation of all or part of the executed program controlling the processor, said verifying being at least partly based on said input data codes and the code computed by the peripheral for each elementary operation performed by the processor, while the processor performs computations only on the functional values of the encoded data.
2. (Original) A computer system according to claim 1, in which the said program is permanent or downloaded.
3. (Original) A computer system according to claim 1, in which the peripheral is single and associated with a host computer to provide security for all of a system having a plurality of computers connected to a common communications medium.
4. (Original) A computer system according to claim 3, in which the host computer is fitted with a safety driver which enables it to dialog with the peripheral and with the other computers.

5. (Original) A computer system according to claim 1, having a plurality of host computers, interconnected by a transmission medium and each provided with a security peripheral.

6. (Original) A computer system according to claim 1, in which the security peripheral or the security peripherals perform security operations only on the inputs/outputs of only some of the processors.

7. (Original) A computer system according to claim 1, having a single security peripheral, connected to a computation assembly constituted by a central unit or a processor and peripherals, said security peripheral having computation means that perform:

- digital security processing; and
- security processing of the inputs/outputs.

8. (Original) A system according to claim 1, characterized in that said security peripheral is designed to make secure an assembly of the system constituted by a smart card, a reader, and one or more computers involved in the processing, and constituting the system, and to generate the interchanges between the smart card and the computer(s).

9. (Original) A system according to claim 1, in which the security peripheral is an ASIC.